SimPassengers — Privacy Notice

Effective date: 01.05.2026 **Last updated:** 09.05.2026

This Privacy Notice explains how ACE Solutions ("we", "us", "our"), operated by Anil Ardahanli with a registered place of business in Turkey, collects, uses, shares, and protects personal data when you use SimPassengers (the "Service"). It covers users in Turkey under the KVKK (Personal Data Protection Law No. 6698) and users in the European Economic Area or the United Kingdom under the GDPR / UK GDPR.

1. Data Controller

The data controller for personal data processed through SimPassengers is:

ACE Solutions / Anil Ardahanli Email: **hello@ace-solutions.io**

For all privacy-related requests use this email address.

2. What we collect and why

We try to collect only what we need to deliver the Service. Below is a complete list of personal data categories and the purposes we use them for.

2.1 Account information

- **Email address, username, name, surname** — to identify you, communicate with you about the Service, and let other users find your public profile (only the username and name are visible publicly when you opt in).
- **Password (hashed)** — to authenticate you. We never store passwords in clear text; we use bcrypt with a per-user salt.
- **Email verification status** — to confirm you control the address you registered with.
- **Avatar URL** (optional) — to personalise your public profile.
- **Public profile preference** — a flag controlling whether your username and flight history are visible to others.

Legal basis (GDPR): performance of a contract — providing the Service you signed up for. **Legal basis (KVKK):** performance of a contract; explicit consent for the public profile flag.

2.2 Hardware fingerprint (HWID)

To prevent unauthorised redistribution of paid licences, the bridge and launcher derive a **composite HWID** from your computer using low-level identifiers: machine identifier, MAC address, computer name, system volume serial, and user domain. The HWID is bound to your account on first sign-in and is checked on later sign-ins.

We store **only the derived HWID and a small, hashed history of its components**. We do not collect a complete inventory of your hardware, software, files, or browsing activity.

You may release ("revoke") the HWID up to three (3) times in any rolling 365-day period from the dashboard. We log the timestamp of each revocation.

Legal basis (GDPR): legitimate interest — protecting the Service and paying users from unauthorised redistribution. **Legal basis (KVKK):** legitimate interest of the data controller.

2.3 Flight telemetry and logs

When the bridge is running and connected to your simulator, it captures information about each

simulated flight, such as:

- origin and destination airports;
- aircraft type and registration;
- route flown, duration, altitude, airspeed and heading samples;
- landing rate, peak g, maximum bank, fuel used;
- in-flight events (turbulence, cabin incidents, scenarios triggered);
- score, achievements, and a summary of cabin notes.

These records are tied to your user account so they can appear in your dashboard, public profile (if enabled), the community feed, and aggregated statistics.

Legal basis (GDPR): performance of a contract. **Legal basis (KVKK):** performance of a contract.

2.4 In-sim PA generation requests

When the in-sim panel asks the bridge to generate a public address announcement, we forward a small context payload (aircraft type, airline, origin and destination ICAO codes and city names, weather phase) to a third-party AI provider (OpenAI or Anthropic) so they can generate the dialogue. We then forward the generated text to **ElevenLabs** to produce audio.

We do **not** include your identity in these requests. The AI providers do not, under their published terms for our usage tier, train on data we send.

Legal basis (GDPR): performance of a contract. **Legal basis (KVKK):** performance of a contract.

2.5 Profile interactions

If you choose to make your profile public, post comments on other profiles, reply to comments, or share an individual flight via a public link, that content becomes visible to anyone with the link. You can remove or hide such content from the dashboard at any time.

Legal basis (GDPR): consent — you actively choose to publish. **Legal basis (KVKK):** explicit consent.

2.6 Purchase records

When you purchase a SimPassengers licence, we receive from **Fungies** a notification that contains your email address, the purchased plan, the order identifier, the amount paid, and the test/live mode flag. We use this to activate your licence ("entitlement"). We do **not** receive your full payment card information; that stays with Fungies and Stripe, who acts as their underlying payment processor.

Legal basis (GDPR): performance of a contract. **Legal basis (KVKK):** performance of a contract.

2.7 Technical and security data

When you use the Service we automatically log:

- **IP address** (truncated where possible) — for rate limiting, abuse prevention, and security investigations;
- approximate timestamps of sign-in, token refresh, and HWID validation;
- error logs and stack traces from the Service when something goes wrong.

We retain these logs for up to **90 days** unless we need to keep them longer to investigate a security incident.

Legal basis (GDPR): legitimate interest — securing the Service. **Legal basis (KVKK):** legitimate interest.

2.8 Mobile companion app (when released)

If you install the SimPassengers mobile app, we will additionally collect:

- a **Firebase Cloud Messaging (FCM) push token** to send you notifications;
- the device platform (iOS / Android);
- your notification preferences.

Push notifications are off by default for follower-related events; you can turn them on or off at any time inside the mobile app.

Legal basis (GDPR): consent for push notifications. **Legal basis (KVKK):** explicit consent.

3. Data we do NOT collect

We do not collect, and we have no commercial reason to collect:

- payment card numbers (these stay with Fungies and Stripe);
- the contents of files on your computer;
- your browsing history outside SimPassengers;
- microphone or camera input;
- precise location data;
- personal data of other people from your computer.

4. Cookies and local storage

The website uses a small number of cookies that are strictly necessary to operate the Service, such as the session cookie and the locale (language) cookie. We do not use third-party advertising cookies or cross-site tracking.

The launcher and bridge store an authentication token in the **Windows Credential Manager** under your local user profile. This is a local secure store, not transmitted to any third party.

5. How long we keep your data

Category	Retention
Account profile	While the account exists. After you delete the account, up to 30 days for backup rotation, then permanent deletion.
Flight logs and telemetry	While the account exists. You may delete individual flights at any time from the dashboard.
HWID + revocation history	While the account exists. Revocation history is kept for 365 days for the rolling-window enforcement, then anonymised.
Purchase records	At least **10 years**, to comply with Turkish tax and accounting law.
Technical / security logs	Up to **90 days**.
Email verification tokens	Until used or **24 hours**, whichever comes first.
Push tokens (mobile)	Until you sign out, the token is invalidated by the operating system, or you delete the app.

6. Who we share data with

We share data only with the providers we need in order to run the Service. The current list is:

- **Amazon Web Services EMEA SARL** (Frankfurt region) — hosting and database for the API and admin console.
- **AWS Amplify** (Frankfurt region) — hosting for the website and admin console front-end.
- **Fungies** (merchant of record) and **Stripe** (Fungies' underlying payment infrastructure) — payment processing, invoicing, and tax/VAT handling.
- **ElevenLabs, Inc.** (United States) — text-to-speech.
- **OpenAI, L.L.C.** (United States) and **Anthropic, PBC** (United States) — large language models for dynamic in-sim dialogue.
- **Google LLC** (United States, when mobile app launches) — Firebase Cloud Messaging push notifications.
- **MongoDB, Inc.** (Atlas) — database hosting.
- **Cloudflare, Inc.** — content delivery and DDoS mitigation.

We do not sell your personal data. We do not share your data for advertising purposes.

We may also disclose data when we are legally required to do so by a competent authority, when needed to enforce our Terms, or to protect the safety of users.

7. International data transfers

Some of our processors are located outside Turkey and outside the European Economic Area, including in the United States. When personal data is transferred to those countries, we rely on the following safeguards:

- **Standard Contractual Clauses** approved by the European Commission, where required;
- the processor's published certifications and binding corporate rules;
- limiting transferred data to what is strictly necessary.

If you would like a copy of the safeguards in place for any specific transfer, write to **anil@ace-solutions.io**.

8. Your rights

Subject to the conditions of the law that applies to you (KVKK in Turkey, GDPR in the EEA, UK GDPR in the United Kingdom), you have the right to:

- **access** the personal data we hold about

you;

- **request correction** of inaccurate or incomplete personal data;
- **request deletion** of your account and personal data, except where we are legally required to keep certain records (for example, billing records for tax purposes);
- **object to or restrict** certain processing;
- **port** your personal data in a structured, machine-readable format;
- **withdraw consent** at any time, for processing that relies on consent (for example, push notifications, public profile).

To exercise any of these rights, write to **anil@ace-solutions.io**. We will reply within **30 days**. If you are not satisfied with our response, you have the right to lodge a complaint with:

- the **Personal Data Protection Authority of Turkey** (Ki ö—6VÂ Verileri Koruma Kurumu — kvkk.gov.tr), if you are based in Turkey;
- the **data protection authority of your country of residence**, if you are based in the EEA or the UK.

9. Children

The Service is not intended for users under **13 years of age**. If you live in the European Economic Area or the United Kingdom, you must be at least **16 years old** (or the age of digital consent in your country) to register. If we learn that we have collected personal data from a child below these ages without verifiable parental consent, we will delete that data.

10. Security

We follow industry-standard security practices, including:

- encrypted transport (TLS) for all traffic between you, our API, and the broker;
- bcrypt password hashing with a per-user salt;
- short-lived authentication tokens with periodic rotation;
- composite HWID binding to detect token theft;
- least-privilege access for our staff;
- separation of test and production environments.

No system is perfectly secure. If we discover a security incident that affects your personal data, we will notify you and the relevant authorities as required by law.

11. Changes to this Notice

We may update this Privacy Notice from time to time. If the changes are material we will notify you by email or through the Service at least **14 days** before the change takes effect. The "Last updated" date at the top of this page always reflects the current version.

12. Contact

For any privacy question, complaint, or rights request:

ACE Solutions / Anil Ardahanli Email: **hello@ace-solutions.io**

End of Privacy Notice.